CLAIMS

We claim:

Claim 1: A method of securely delivering data, comprising the steps of:

creating a container having electronic content and a container identifier;

encrypting at least one data block of the electronic content using a symmetric encryption technique and encrypting a header associated with a first data block of the electronic content using an asymmetric encryption technique, the header including a symmetric decryption key; and

re-keying the header using data associated with a user or a user's device to lock at least a portion of the electronic content to the user or the user's device,

wherein the locked at least a portion of the electronic content can only be decrypted and accessed by the user or on the user's device when the user or user's device has been authenticated against at least the container identifier.

Claim 2: A system for securely delivering data, comprising at least one component to:

create a container having electronic content and a container identifier;

encrypt at least one data block of the electronic content using a symmetric encryption technique and to encrypt a header associated with a first data block of the electronic content using an asymmetric encryption technique, the header including a symmetric decryption key; and

re-key the header using data associated with a user or a user's device to lock at least a portion of the electronic content to the user or the user's device,

wherein the locked at least a portion of the electronic content can only be decrypted and accessed by the user or on the user's device when the user or user's device has been authenticated against at least the container identifier.

Claim 3: A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product includes at least one component to:

create a container having electronic content and a container identifier;

determining at least one data block for partitioning the electronic content;

encrypt the at least one data block of the electronic content using a symmetric encryption technique and to encrypt a header associated with a first data block of the electronic content using an asymmetric encryption technique, the header including a symmetric decryption key;

re-key the header using data associated with a user or a user's device to lock at least a portion of the electronic content to the user or the user's device, wherein the locked at least a portion of the electronic content can only be decrypted and accessed by the user or on the user's device when the user or user's device has been authenticated against at least the container identifier; and

decrypt the locked portion of the electronic content when the user or user's device has been authenticated.